



The Argument for Public, Emulator-based SCADA/DCS Testbeds

Anthony D. Joseph

Terry V. Benzel

**National Workshop on Beyond SCADA:
Networked Embedded Control for Cyber
Physical Systems, November 8, 2006**



Public SCADA/DCS Testbed Motivation



- SCADA/DCS design, development, and testing
 - Multi-year design and replacement cycles
 - Significant capital and time investments
- Inadequate deployment of security technologies
 - Over 10+ yrs of network security research investment
 - Significant opportunities for vulnerability exploitation
- Lack of public experimental infrastructure
 - Testing and validation occurs mostly at small scales
 - Lack of objective test data, traffic and metrics

Physical Testbeds



Pros

- Actual hardware and systems provide accurate results
- Can explore interactions between components

Cons

- Very expensive to build and maintain
- High cost limits numbers of testbeds
- Hard to change
- Single user/exclusive access mode of operation

Cyber Testbeds



Pros

- Relatively inexpensive to build and maintain
- More, larger testbeds feasible
- Easy to dynamically change
- Multi-user/shared/remote access

Cons

- Acquiring/building emulators is a challenge
- Emulation results verification is hard
- Performing time sensitive experiments is challenging

Combined Physical and Cyber Testbeds



- Combine aspects of both types of testbeds
 - Commodity HW and limited amts of “real” HW
 - Federate together multiple testbeds into larger one
- Use FPGA-based hardware emulators
 - Research Accelerator for MultiProcessing (RAMP)
 - 1,000 200-300 Mhz FPGA-based CPUs
 - Many 10GE I/O ports
 - ~\$100K for 8U box at 1.5KW
- Must be open to all researchers

